Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Paula W. Klimach** **Group Art Unit 2135**	Facsimile No.: **571/273-8300**
From: Jennifer Pilcher Legal Assistant to Wayne Bailey	No. of Pages Including Cover Sheet: **30**

Message:

Enclosed herewith:

- Transmittal Document; and
- Appeal Brief.

Re: Application No. 09/874,813
Attorney Docket No: **YOR920010390US1**

Date: Tuesday, January 03, 2006

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Mraz**

Serial No.: **09/874,813**

Filed: **June 5, 2001**

For: **High Volume Secure Internet Server**

§ Group Art Unit: **2135**

§

§ Examiner: **Klimach, Paula W.**

§

§ Attorney Docket No.: **YOR920010390US1**

§

35526
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on January 3, 2006.

By: Jennifer Pilcher

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37)

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 50-0510. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 50-0510. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 50-0510.

Respectfully submitted,

Gerald H. Glanzman
Registration No. 25,035
Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEYS FOR APPLICANT

Docket No. YOR920010390US1 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Mraz** §
§ Group Art Unit: **2135**
Serial No. **09/874,813** §
§ Examiner: **Klimach, Paula W.**
Filed: **June 5, 2001** §
§
For: **High Volume Secure Internet Server** §
§

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on January 3, 2006.

By: Jennifer Pilcher
Jennifer Pilcher

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on November 3, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

01/04/2006 TL0111 00000055 500510 09874813
01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, New York.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-56

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: none
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-56
4. Claims allowed: none
5. Claims rejected: 1-56
6. Claims objected to: none

C. CLAIMS ON APPEAL

The claims on appeal are: 1-56

STATUS OF AMENDMENTS

An amendment after final was filed by Appellants on August 3, 2005, and was indicated as being entered by the Examiner in an Advisory Action dated August 19, 2005.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

Data processing using networks for accessing multiple computers is becoming ubiquitous. Many networks such as the internet are publicly accessible, and data exchanged across such a network can easily be compromised if not secured in some fashion. Cryptography is often used to protect data on a network from inadvertent or malicious access by undesired systems or third parties. As systems become larger and larger, the overhead associated with cryptographic operations can become significant, and adversely affect overall system performance. There exists a need to provide a system that is capable of efficiently handling/serving a large number of transactions in a secure fashion.

Claim 1 is directed to a technique for serving secure network transactions using a distributed data processing system having three classes of servers – (1) an in-line crypto engine for performing encryption and decryption, (2) a dedicated handshake server for establishing cryptographic parameters, and (3) a transaction server for servicing the transactions. By use of three different classes of servers, efficiency and scalability are provided by distributing the work load involved in a secure network communication amongst these classes of servers depending upon the particular action that needs to be performed. For example, the in-line crypto engine can be used for performing the actual encryption/decryption of data, the handshake server can be used for establishing the cryptographic parameters to be used by the in-line crypto engine, and the transaction server can be used for actually servicing the transaction. This allows for improved scalability, as the system can be scaled so that more resource-intensive operations, such as the handshaking procedure, can be distributed across a larger number of servers than less resource-intensive operations. In addition, an added benefit is realized by having transaction servers that operate on unencrypted data so such a packet-sniffing firewall or caching system may be implemented, where such features were previously unavailable to secure Internet sites.

Specifically, Claim 1 is directed to a method of servicing secure transactions in a network, including steps of establishing cryptographic parameters in a handshake engine, servicing a transaction in a transaction server using unencrypted data, and utilizing an inline

crypto engine and the cryptographic parameters established by the handshake engine to perform at least one of encryption associated with transmitted data and decryption associated with transmitted data, the inline crypto engine having capability for performing at least one of encryption and decryption of data (Specification page 16, line 10 – page 17, line 3; Figure 11, all blocks).

B. CLAIM 19 - INDEPENDENT

Claim 19 is a program product claim corresponding to method Claim 1, and the summary of Claim 1 is applicable for Claim 19, and thus is hereby incorporated by reference.

C. CLAIM 38 - INDEPENDENT

Claim 38 is an apparatus claim corresponding to method Claim 1, and the summary of Claim 1 is applicable for Claim 38, and thus is hereby incorporated by reference.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-56)

Claims 1-56 stand rejected under 35 U.S.C. § 103(a) as being obvious over Jardin (6,681,327) in view of Matsumoto et al. ("Speeding Up Secret Computations with Insecure Auxiliary Devices").

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-56)

A.1. Claims 1-3, 5-15, 18-21, 23-33, 36-40, 42-51 and 53-56

Even when the references have been improperly combined (as further shown below), Appellants show that there is still at least one missing claimed feature not taught or suggested by the cited references, and thus a proper prima facie case of obviousness has not been established with respect to Claim 1[1]. In particular, none of the cited references teach or suggest utilizing one engine (an online crypto engine) to perform encryption or decryption *using cryptographic parameters established by another engine* (a handshake engine). Claim 1 specifically recites "utilizing an *inline crypto engine* and the *cryptographic parameters established by the handshake engine* to perform at least one of encryption associated with transmitted data and decryption associated with transmitted data, the inline crypto engine having capability for performing at least one of encryption and decryption of data". In rejecting this aspect of Claim 1, the Examiner cites Matsumoto's server as teaching the claimed inline crypto engine, and Jardin's broker 120 as teaching the claimed handshake engine. Because these two devices (Matsumoto's server and Jardin's broker) are described in two separate references, it necessarily follows that there is no teaching or suggestion of the claimed co-action between such devices (as they are both described separately in their respective individual teachings, and thus there is no teaching of any synergistic co-action between these separately described devices), and in particular there is no teaching or suggesting of using parameters establish by one of these devices (Jardin's broker) by the other of these devices (Matsumoto's server). Restated, Claim 1 is not an apparatus claim that merely recites two engines, but rather is a method claim that recites synergistic co-action between two engines as a part of the claimed method. In finally rejecting Claim 1, the Examiner states:

---

[1] In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the Applicant. *Id.* To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974) (emphasis added by Appellant).

> "Although Jardin discloses the decryption and encryption of communication packets between the server and client (Fig. 3 steps 330-338) the encryption and decryption performed with the parameters established by the handshake engine (Fig. 4), Jardin does not disclose an inline crypto engine performing the earlier mentioned encryption and decryption.
>
> Matsumoto discloses a system wherein a server, inline crypto engine performs the function of the secret computation, encryption and decryption, on behalf of a client device; therefore the inline crypto engine having capability for performing at least one of encryption and decryption of data (page 497, Introduction, paragraph 3). Since Matsumoto performs encryption and decryption then it follows that Matsumoto has the capability of performing at least one of encryption and decryption."

Notably absent from such assertion is any statement with respect to using one engine (an online crypto engine) to perform encryption or decryption *using cryptographic parameters established by another engine* (a handshake engine). Claim 1 specifically recites:

> "utilizing an *inline crypto engine* and the *cryptographic parameters established by the handshake engine* to perform at least one of encryption associated with transmitted data and decryption associated with transmitted data, the inline crypto engine having capability for performing at least one of encryption and decryption of data".

As can be seen, the inline crypto engine performs encryption or decryption associated with transmitted data *using cryptographic parameters established by another engine* (the handshake engine). The Examiner merely alleges that Matsumoto has the capability of performing encryption/decryption, but does not allege any teaching/suggestion of performing such operation using cryptographic parameters established by a different engine. Thus, a prima facie case of obviousness has not been established with respect to Claim 1, as there is at least one missing

claimed element not taught/suggested by the cited references (or even alleged to be taught/suggested by the cited references) and Claim 1 has therefore been erroneously rejected[2].

Appellants further urge that there would have been no motivation to one of ordinary skill in the art at the time of the present invention to include an additional device such as Matsumoto's server to provide an encrypt/decrypt function to the teachings of Jardin, *as Jardin already possesses processing blocks and associated functionality to perform encryption and decryption* (Jardin Broker 120 of FIG 1; col. 4, line 35 – col. 6, line 3). In addition, Jardin requires that such encryption be performed directly by a broker server such that decrypted packets can easily be buffered and redirected to an intended recipient server (Jardin col. 2, line 56 – col. 3, line 3). Thus, a person of ordinary skill in the art would not have been motivated to combine Matsumoto's teachings with those of Jardin, as (1) it would result in duplicate functionality (which is unnecessary and thus increases system cost and complexity such as associated overhead that would necessarily be required to manage this passing-off of functionality to another server), and (2) it would defeat an expressed desire by Jardin to perform encryption/decryption by the handshake broker itself. Therefore, the only motivation for combining the teachings of Matsumoto with the teachings of Jardin must therefore be coming from Appellants' own patent specification, which is *improper hindsight analysis*. It is error to reconstruct the patentee's claimed invention from the prior art by using the patentee's claims as a "blueprint". When prior art references require selective combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight obtained from the invention itself. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 227 USPQ 543 (Fed. Cir. 1985). There is simply no reason for the combination other than hindsight obtained from the present invention, and thus Claim 1 is further shown to have been erroneously rejected under 35 USC 103(a).

Still further with respect to Claim 1, because of Jardin's desire to use a common broker to provide *both* (i) handshake and decryption for a client (column 4, line 35 – column 6, line 3), *and* (ii) handshake and encryption for a back-end transaction server (column 7, lines 6-19), there would have been no motivation to somehow separate the handshake and encryption/decryption

[2] If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In the absence of a proper *prima facie* case of obviousness, an Appellant who complies with the other statutory requirements is entitled to a patent. *See In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992).

functionality and still provide such dual-purpose functionality by a common broker - as expressly desired by the teachings of the cited Jardin reference – further evidencing no motivation to modify the teachings of Jardin in accordance with the claimed invention. The fact that a prior art device could be modified so as to produce the claimed device is not a basis for an obviousness rejection unless the prior art suggested the desirability of such a modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). There is simply no desire or suggestion of any desire to modify Jardin in accordance with the claimed invention recited in Claim 1, and thus Claim 1 is further shown to have been erroneously rejected under 35 USC 103(a).

The claimed co-action between the handshake engine and the inline crypto engine advantageously provides an ability to separate the handshaking functionality from the encryption/decryption functionality to improve performance, as the handshaking functionality is inherently much slower to perform (Specification page 13, lines 13-20). Per the present invention, this handshake functionality can be performed by a separate handshake engine, thus offloading the handshake operations that would otherwise hinder the performance of the encryption/decryption engine (Specification page 14, lines 20-22).

A.2. Claims 4, 22 and 41

Appellants initially show error in the rejection of Claim 4 (and similarly for Claims 22 and 41) for reasons given above regarding Claim 1 (of which Claim 4 depends upon).

Further with respect to Claim 4, Appellants urge that none of the cited references teach or suggest the claimed feature of "wherein the establishing step includes handing off a network connection from the transaction server to the handshake engine such that the handshake engine can establish the cryptographic parameters with a client coupled to the network". As can be seen, the network connection is handed off from the transaction server to the handshake engine such that this handshake engine can establish the cryptographic parameters with a client (such cryptographic parameters being used by the inline crypto engine – a different engine – for the actual encryption/decryption operation). In rejecting Claim 4, the Examiner cites Jardin's Figure 3, blocks 340, 342, 344 and 346 as teaching this claimed feature. Appellants urge that Jardin's Figure 3 describes the internal process flow between a broker 120 and a transaction server 130 (Jardin column 6, line 4 – column 7, line 56). Notably, it is Jardin's broker (which allegedly reads on the claimed handshake engine) that hands-off the communication link to a transaction

server (Jardin, column 6, lines 39-41), which is just the opposite of what is recited in Claim 4, where the network connection is handed-off *from* the transaction server (alleged to by Jardin's transaction server 130) *to* the handshake engine (alleged to be Jardin's broker 120). Per Claim 4 (as depicted in the preferred embodiment in Appellants' Figure 9), the transaction server itself has a network connection to the network (as established by the process depicted in Figure 8 - note in particular the heavy line from the client/Internet to the transaction server which bypasses the handshake engine), and thus has a network connection that can be handed off to the handshake engine 900. This is a substantially different process and resulting data flow from the teachings of the cited references. Jardin teaches a network connection being made by a broker, with a back-end transaction server *which solely communicates with the broker* (col. 7, line 57 – col. 8, line 26; Fig. 4, block 410). Per Claim 4, the *transaction broker itself has a network connection for accessing the network*, and this network connection is *handed off to the handshake engine* (alleged to be Jardin's broker 120) so that the handshake engine can establish the cryptographic parameters with the network-connected client. Thus, Claim 4 is further shown to have been erroneously rejected, as there is an additional claimed feature not taught or suggested by the cited references.

This distinction can also be seen by a careful review of the cited Jardin teachings at Figure 3, blocks 340, 342, 344 and 346 (which are being cited as teaching all features of Claim 4), which require the broker to have *already established encryption parameters with the client* prior to any broker-to-server communication (col. 4, lines 35-58 and Figure 2; and in particular col. 6, lines 4-9). The can also be seen in the cited block 340 of Jardin Figure 3, where the broker decrypts packets from the client so the cryptographic parameters have already been established with the client, and thus there would be no reason to hand-off the connection from the transaction server 130 to broker 120 in order to establish cryptographic parameters with a client, as they have already been established. This further evidences error in the Examiner's rejection of Claim 4.

A.3. Claims 16, 17, 34, 35

Appellants initially show error in the rejection of Claims 16 and 17 (and similarly for Claims 34 and 35) for reasons given above regarding Claim 1 (of which Claims 16 and 17 depend upon).

Further with respect to Claims 16 and 17, such claims specify that the inline crypto engine receives/transmits data from/to the network. In other words, the claimed inline crypto engine is located at the front-end of the system. In contrast, Matsumoto's server (which is alleged to read on the claimed inline crypto engine) is a back-end processor. In rejecting Claim 16, the Examiner cites Jardin's part 430 of Figure 4 as teaching this claimed feature. Appellants urge that this further evidences the improper hindsight analysis being used by the Examiner in combining the references. Why would a person of ordinary skill in the art add a back-end crypto server (as alleged to be taught by Matsumoto) if the Jardin system being modified already has a front-end crypto server? Again, this duplication of functionality is unwieldy, costly, complex, and quite simply would have been illogical to a person of ordinary skill in the art.

The Examiner is also impermissibly changing the interpretation of the cited references. In one instance, Matsumoto's server is being stated as teaching the claimed inline crypto engine (see page 4 of the present office action, where it states "Jardin does not disclose an inline crypto engine" in rejecting Claim 1), and yet the Examiner states in rejecting Claim 16 "Jardin discloses a system further comprising: receiving the transmitted data from the network by the inline crypto engine". If Jardin does not disclose an inline crypto engine (as admitted by the Examiner in the rejection of Claim 1), it necessarily follows that Jardin does not disclose receiving data from the network *by such missing inline crypto engine.* Thus, Claims 16 and 17 are further shown to not be obvious in view of the cited references, as there are further missing claimed features not taught or suggested by the cited references.

A.4. Claim 52

Appellants initially show error in the rejection of Claim 52 for reasons given above regarding Claim 38 (of which Claim 52 depends upon).

Further with respect to Claim 52, Appellants urge that none of the cited references teach or suggest the claimed feature of "wherein the at least one transaction server receives a request to establish the cryptographic parameters; and responsive to the at least one transaction server's receiving the request, the at least one handshake engine performs the establishing step". In rejecting Claim 52, the Examiner alleges that Jardin teaches the features of Claim 52 at Jardin's Figure 2. Appellants urge that Jardin's Figure 2 is with respect to communication between a client 110 and a broker 120, and provides no teaching/suggestion of *any transaction server*, and

in particular provides no teaching/suggestion of a transaction server that receives a request to establish the cryptographic parameters, as expressly recited in Claim 52. The Examiner has equated the claimed transaction server with Jardin's elements 130a, 130b and 130c of Figure 1 (per page 4 of the present Office Action, which cites Jardin col. 8, lines 5-17 as teaching the claimed transaction server). Neither this transaction server, nor its operations, is depicted in Jardin's Figure 2, and therefore the Examiner's citation of Jardin's Figure 2 as teaching the claimed transaction server features recited in Claim 52 is shown to be in error. Thus, Claim 52 is further shown to not be obvious in view of the cited references.

Still further with respect to Claim 52, it is urged that none of the cited references teach or suggest the claimed feature of "responsive to the at least one transaction server's receiving the request, the at least one handshake engine performs the establishing step". As can be seen, one server (transaction server) receives a request to establish cryptographic parameters, and another engine (handshake engine) actually establishes the cryptographic parameters responsive to the transaction server receiving the request. Jardin's Figure 2, which is being cited as teaching all features of Claim 52, merely shows a transaction between a client (which is not alleged to teach either the claimed transaction server or the handshake engine) and a broker (which is alleged to teach the claimed handshake engine, per page 4 of the present Office Action, citing Jardin column 4, lines 35-58). Thus, Jardin's Figure 2 does not depict or otherwise teach/suggest (1) any type of transaction server, or (2) any co-action between a (missing) transaction server and handshake engine, as expressly recited in Claim 52. Thus, Claim 52 is further shown to have been erroneously rejected, as there are missing claimed features not taught or suggested by the cited references.

In summary, the Examiner's combination of references would result in a system having duplicate/redundant functionality without purpose, thus evidencing an improper combination of references. Even with such improper combination, the synergistic co-action between the claimed handshake engine, transaction server, and inline crypto engine is not taught or otherwise suggested, further evidencing non-obviousness of the present invention. It is therefore requested that the Board reverse the rejection of all pending claims.

Gerald H. Glanzman
Reg. No. 25,035
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method of servicing secure transactions in a network, comprising:

establishing cryptographic parameters in a handshake engine;

servicing a transaction in a transaction server using unencrypted data;

utilizing an inline crypto engine and the cryptographic parameters established by the handshake engine to perform at least one of encryption associated with transmitted data and decryption associated with transmitted data, the inline crypto engine having capability for performing at least one of encryption and decryption of data.

2. The method of claim 1, wherein the inline crypto engine performs decryption on the transmitted data to obtain the unencrypted data.

3. The method of claim 1, wherein the inline crypto engine performs encryption on the unencrypted data to obtain the transmitted data.

4. The method of claim 1, wherein the establishing step includes handing off a network connection from the transaction server to the handshake engine such that the handshake engine can establish the cryptographic parameters with a client coupled to the network.

5. The method of claim 1, wherein the servicing step includes handing off a network connection from the handshake engine to the transaction server.

6. The method of claim 1, wherein the establishing step includes performing a Secure Sockets Layer (SSL) handshake procedure.

7. The method of claim 1, wherein the establishing step includes performing a Transport Layer Security handshake procedure.

8. The method of claim 1, wherein the transaction is returning at least one of a data file and streaming data.

9. The method of claim 8, wherein the streaming data includes at least one of audio data and video data.

10. The method of claim 8, wherein the data file includes at least one of a hypertext page and a structured data file.

11. The method of claim 1, wherein the transaction is submitting information taken from a form.

12. The method of claim 1, wherein the cryptographic parameters include at least one cryptographic key.

13. The method of claim 12, wherein the at least one cryptographic key includes at least one of a public key and a private key.

14. The method of claim 1, further comprising:

notifying the inline crypto engine of the cryptographic parameters.

15. The method of claim 12, further comprising:

receiving a request to establish the cryptographic parameters; and

responsive to receiving the request, performing the establishing step.

16. The method of claim 1, further comprising:

receiving the transmitted data from the network by the inline crypto engine.

17. The method of claim 1, further comprising:

transmitting the transmitted data to the network by the inline crypto engine.

18. The method of claim 1, wherein the unencrypted data is a request to perform the transaction.

19. A computer program product in at least one computer readable medium for servicing secure transactions in a network, comprising instructions for:

establishing cryptographic parameters in a handshake engine;

servicing a transaction in a transaction server using unencrypted data;

utilizing an inline crypto engine and the cryptographic parameters established by the handshake engine to perform at least one of encryption associated with transmitted

data and decryption associated with transmitted data, the inline crypto engine having capability for performing at least one of encryption and decryption of data.

20. The computer program product of claim 19, wherein the inline crypto engine performs decryption on the transmitted data to obtain the unencrypted data.

21. The computer program product of claim 19, wherein the inline crypto engine performs encryption on the unencrypted data to obtain the transmitted data.

22. The computer program product of claim 19, wherein the instructions for establishing include instructions for handing off a network connection from the transaction server to the handshake engine such that the handshake engine can establish the cryptographic parameters with a client coupled to the network.

23. The computer program product of claim 19, wherein the instructions for servicing include instructions for handing off a network connection from the handshake engine to the transaction server.

24. The computer program product of claim 19, wherein the instructions for establishing include instructions for performing a Secure Sockets Layer (SSL) handshake procedure.

25. The computer program product of claim 19, wherein the instructions for establishing include instructions for performing a Transport Layer Security handshake procedure.

26. The computer program product of claim 19, wherein the transaction is returning at least one of a data file and streaming data.

27. The computer program product of claim 26, wherein the streaming data includes at least one of audio data and video data.

28. The computer program product of claim 26, wherein the data file includes at least one of a hypertext page and a structured data file.

29. The computer program product of claim 26, wherein the transaction is submitting information taken from a form.

30. The computer program product of claim 19, wherein the cryptographic parameters include at least one cryptographic key.

31. The computer program product of claim 30, wherein the at least one cryptographic key includes at least one of a public key and a private key.

32. The computer program product of claim 19, further comprising instructions for:

notifying the inline crypto engine of the cryptographic parameters.

33. The computer program product of claim 30, further comprising instructions for:

receiving a request to establish the cryptographic parameters; and

responsive to receiving the request, performing the establishing step.

34. The computer program product of claim 19, further comprising instructions for:

receiving the transmitted data from the network by the inline crypto engine.

35. The computer program product of claim 19, further comprising instructions for:

transmitting the transmitted data to the network by the inline crypto engine.

36. The computer program product of claim 19, wherein the unencrypted data is a request to perform the transaction.

37. The computer program product of claim 19, wherein the unencrypted data is a hypertext page.

38. A distributed data processing system for servicing secure transactions in a network, comprising:

at least one inline crypto engine in communication with the network, wherein the at least one inline crypto engine includes at least one processor for performing at least one of encryption and decryption of data;

at least one transaction server in communication with the at least one inline crypto engine, wherein the at least one transaction server includes at least one processor; and

at least one handshake engine in communication with the at least one transaction server and the at least one inline crypto engine, wherein the at least one handshake engine includes at least one processor,

wherein the at least one handshake engine establishes cryptographic parameters,

the transaction server services a transaction using unencrypted data, and

the at least one inline crypto engine utilizes the cryptographic parameters established by the handshake engine to perform at least one of encryption associated with the transmitted data and decryption associated with transmitted data.

39. The distributed data processing system of claim 38, wherein the at least one inline crypto engine performs decryption on the transmitted data to obtain the unencrypted data.

40. The distributed data processing system of claim 38, wherein the at least one inline crypto engine performs encryption on the unencrypted data to obtain the transmitted data.

41. The distributed data processing system of claim 38, wherein establishing the cryptographic parameters includes handing off a network connection from the at least one transaction server to the at least one handshake engine such that the handshake engine can establish the cryptographic parameters with a client coupled to the network.

42. The distributed data processing system of claim 38, wherein servicing the transaction includes handing off a network connection from the at least one handshake engine to the at least one transaction server.

43. The distributed data processing system of claim 38, wherein establishing the cryptographic parameters includes performing a Secure Sockets Layer (SSL) handshake procedure.

44. The distributed data processing system of claim 38, wherein establishing the cryptographic parameters includes performing a Transport Layer Security handshake procedure.

45. The distributed data processing system of claim 38, wherein the transaction is returning at least one of a data file and streaming data.

46. The distributed data processing system of claim 45, wherein the streaming data includes at least one of audio data and video data.

47. The distributed data processing system of claim 45, wherein the data file includes at least one of a hypertext page and a structured data file.

48. A method for using the distributed data processing system of claim 38, comprising steps of:

receiving, from a client coupled to the network, a request by one inline crypto engine of the at least one inline crypto engine;

determining whether the received request is encrypted;

if the received request is encrypted, decrypting the received request by the one inline crypto engine and passing the decrypted received request to one transaction server of the at least one transaction server;

if the received request is not encrypted, passing the received request to the one transaction server;

determining whether a handshake procedure must be performed, and if so, handing off a network connection from the one transaction server to one handshake engine of the at least one handshake engine such that the one handshake engine can establish the cryptographic parameters with the client.

49. The distributed data processing system of claim 38, wherein the cryptographic parameters include at least one cryptographic key.

50. The distributed data processing system of claim 49, wherein the at least one cryptographic key includes at least one of a public key and a private key.

51. The distributed data processing system of claim 38, wherein the at least one handshake engine notifies the inline crypto engine of the cryptographic parameters.

52. The distributed data processing system of claim 49, wherein the at least one transaction server receives a request to establish the cryptographic parameters; and responsive to the at least one transaction server's receiving the request, the at least one handshake engine performs the establishing step.

53. The distributed data processing system of claim 38, wherein the unencrypted data is a request to perform the transaction.

54. The distributed data processing system of claim 38, further comprising a network dispatcher coupled between the at least one inline crypto engine and the at least one transaction server.

55. The distributed data processing system of claim 38, wherein the at least one transaction server, the at least one inline handshake engine, and the at least one inline crypto engine operate concurrently.

56. The distributed data processing system of claim 38, wherein the at least one transaction server, the at least one inline handshake engine, and the at least one inline crypto engine operate asynchronously.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.